IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for detecting intrusions on a host, comprising:
   a) a sensor for collecting information including events and timestamps from a logfile; and
   b) an analysis engine configured to identify a backward ~~and forward~~ time step[[s]] in the logfile by identifying a first entry for which an associated first log entry time is earlier in time than a second log entry time associated with a second log entry entered in the log prior to the first entry, correlate the backward time step[[s]] with an event[[s]], and assign a suspicion value to [[an]] the event.

2. (Original) The system as recited in claim 1, wherein the analysis engine is configured to identify a time step as forward if a timestamp of an entry in the logfile is later than an preceding entry in the logfile, and identify a time step as backward if a timestamp of an entry in the logfile is earlier than an preceding entry in the logfile.

3. (Original) The system as recited in claim 1, wherein the analysis engine is further configured to use expected activity level in the directory to determine the suspicion value.

4. (Original) The system as recited in claim 1, further comprising a second sensor for collecting information including events and timestamps from a second logfile.

5. (Original) The system as recited in claim 4, wherein the analysis engine is configured to correlate a time step in the logfile with an event in the second logfile.

6. (Original) The system as recited in claim 1, wherein the analysis engine is further configured to filter out expected time steps from further analysis.

7. (Original) The system as recited in claim 6, wherein the analysis engine is configured to filter out expected backward time steps by correlating them to Network Time Protocol adjustments.

8. (Original) The system as recited in claim 6, wherein the analysis engine is further configured to compute an expected time drift resulting from a Network Time Protocol adjustment, and compare a forward time step in the logfile with the expected time drift.

9. (Original) The system as recited in claim 8, wherein the analysis engine is further configured to compute a standard deviation of the expected time drift.

10. (Original) The system as recited in claim 9, wherein the analysis engine is further configured to label time steps with weighted distributions.

11. (Original) The system as recited in claim 1, further comprising a user interface, and wherein the analysis engine is configured, upon correlating a time step to a record of an event in a logfile, to present the record to a user for labeling as to suspicion value.

12. (Original) The system as recited in claim 11, wherein the analysis engine is further configured to propagate the suspicion value to related events.

13. (Canceled)

14. (Canceled)

15. (Canceled)

16. (Currently Amended) A method for detecting intrusions on a host, comprising the steps of:

a) collecting information including events and timestamps from a logfile;

b) identifying a backward ~~and forward~~ time step[[s]] in the logfile by identifying a first entry for which an associated first log entry time is earlier in time than a second log entry time associated with a second log entry entered in the log prior to the first entry;

c) correlating the backward ~~and forward~~ time step[[s]] with an event[[s]]; and

d) assigning a suspicion value to the [[an]] event.

17. (Currently Amended) A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of:

a) collecting information including events and timestamps from a logfile;

b) identifying a backward ~~and forward~~ time step[[s]] in the logfile by identifying a first entry for which an associated first log entry time is earlier in time than a second log entry time associated with a second log entry entered in the log prior to the first entry;

c) correlating the backward ~~and forward~~ time step[[s]] with an event[[s]]; and

d) assigning a suspicion value to the [[an]] event.

INTERVIEW SUMMARY UNDER 37 CFR §1.133 AND MPEP §713.04

A telephonic interview in the above-referenced case was conducted on April 6, 2005 between the Examiner and the Applicants' undersigned representative. The Final Office Action mailed on January 5, 2005 was discussed. Specifically, the rejections of claim 1 in light of Porras et al. (U.S. Patent No. 6,704,874 B1) and the proposed amendments set forth herein were discussed with the intent to place the claims in better condition for allowance or appeal. The Applicants wish to thank the Examiner for his time and attention in this case.